

00

## Caller authentication system for telecommunication networks e.g. in home banking, shopping

Publication number: DE4406590

Publication date: 1995-09-07

Inventor: SIMON WERNER DIPL ING (DE)

Applicant: DEUTSCHE BUNDESPOST TELEKOM (DE)

Classification:

- international: G06Q20/00; G07F7/10; H04M3/38; G06Q20/00;  
G07F7/10; H04M3/38; (IPC1-7): H04L9/32; G07C9/00;  
H04M3/42; H04M11/00

- european: G06Q20/00; G07F7/10D4; H04M3/38A

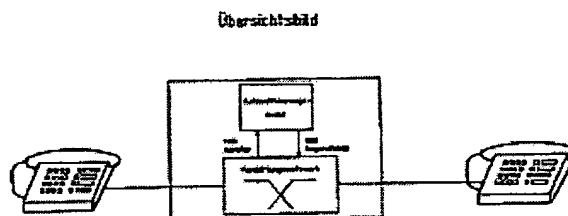
Application number: DE19944406590 19940301

Priority number(s): DE19944406590 19940301

Report a data error here

### Abstract of DE4406590

The authentication system involves embedding the authentication process within the network rather than in the end user devices. The network provider sets the characteristic parameters of the user layer of the authentication process and includes them as part of the network service. Compatible modes of authentication and the devices required for their implementation are provided whenever a connection is made between caller and destination. The authentication process is adapted for the specific relationship between parties to an individual connection.



Data supplied from the esp@cenet database - Worldwide



FA

①9 BUNDESREPUBLIK  
DEUTSCHLAND



DEUTSCHES  
PATENTAMT

⑫ Offenlegungsschrift  
⑩ DE 44 06 590 A 1

⑤1 Int. Cl. 6:  
H 04 L 9/32  
H 04 M 11/00  
H 04 M 3/42  
G 07 C 9/00

②1 Aktenzeichen: P 44 06 590.6  
②2 Anmeldetag: 1. 3. 94  
④3 Offenlegungstag: 7. 9. 95

DE 44 06 590 A 1

⑦1 Anmelder:  
Deutsche Bundespost Telekom, 53175 Bonn, DE

⑦2 Erfinder:  
Simon, Werner, Dipl.-Ing., 64289 Darmstadt, DE

⑤6 Für die Beurteilung der Patentfähigkeit  
in Betracht zu ziehende Druckschriften:

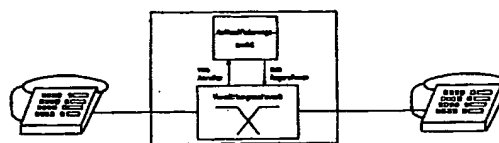
DE	40 27 735 A1
DE	39 22 642 A1
FR	26 19 941
US	52 02 921
US	51 63 086
US	50 68 894
US	50 48 085
US	50 36 461
US	48 97 875
US	48 02 218
EP	04 51 695 A2
EP	5 73 245 A2
WO	94 01 963

ASANO, Tomoyuki: Methods to Securely Realize  
Caller-Authenticated and Callee-Specified  
Telephone Calls. In: JEICE Trans, Fundamen-  
tals, Vol. E76-A, No. 1, Jan. 1993, S. 88-95;  
ALLERBECK, Mechthild;  
FISCHER, Norbert: Mobile Kommunikation mit  
HICOM-Chipkarte. In: telcom report 9, 1986, H. 4,  
S. 270-273;  
ARNDT, Gerhard;  
LUEDER, Reinhard: Bewegungsfreiheit in allen  
Netzen. In: Siemens telcom re- port 2/93, S. 67-69;  
GABEL, J.: Die Chipkarte im Funktelefonnetz C. In:  
ntz Bd. 41, 1988, H. 10, S. 586-589;

⑤4 System zur Authentifizierung von Anrufern

⑤7 Bei bekannten Systemen erfolgt die Authentifizierung in  
den Endstellen oder in diesen zugeordneten speziellen  
Schnittstellen. Bekannte Telekommunikationsnetze ermögli-  
chen keine persönliche Identifizierung, sondern höchstens  
den Anschluß des Anrufers. Für eine Authentifizierung muß  
er zusätzlich ausgerüstet sein.  
Eine weitergehende Möglichkeit der Authentifizierung wird  
erreicht, indem die bestimmenden Parameter der Benutzer-  
oberfläche des Verfahrens der Authentifizierung vom Netz-  
betreiber festgelegt werden, der auch die Vorrichtungen  
hierzu, dem Vermittlungsnetzwerk zugeordnet, zur Verfü-  
gung stellt.  
Mit dem veränderten System wird eine wesentlich erweiter-  
te Akzeptanz der Authentifizierung bei den Anrufern er-  
reicht, die für seltene Anwendungen keinen erhöhten End-  
stellen- oder Schnittstellenaufwand treiben möchten.

Übersichtsbild



DE 44 06 590 A 1

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

BUNDESDRUCKEREI 07. 95 508 036/77

4/31

Die Erfindung bezieht sich auf ein im Oberbegriff des Patentanspruchs 1 näher definiertes System zur Authentifizierung von Anrufern. Von solchen Systemen, die bestimmten sicherheitsrelevanten Endeinrichtungen oder für solche speziell vorgesehenen Schnittstellen zugeordnet werden, ist eine Vielzahl in der Literatur beschrieben.

Telekommunikationsnetze, vorzugsweise Telefonnetze, erlauben keine persönliche Identifizierung des Anrufers beim Angerufenen. Moderne zentralgesteuerte Netze, wie z. B. das ISDN, identifizieren lediglich optional den anrufenden Anschluß durch Übermittlung von dessen Rufnummer. Für die Fälle, in denen eine weitergehende Identifizierung der Person des Anrufers gewünscht wird, müssen Absprachen hinsichtlich Benutzeroberfläche und Übertragungsverfahren für eine Authentifizierung des Anrufers über das Netz zwischen den Kommunikationspartnern, dem Netzbetreiber hinsichtlich des Übertragungsverfahrens, und den Anbietern von Endeinrichtungen hinsichtlich deren Eignung getroffen werden.

Als besonderer Nachteil ist zu erachten, daß jeder potentielle Anrufer von Diensten mit Authentifikationsbedarf solche speziellen Einrichtungen bzw. Schnittstellen wie z. B. Kunde/Bank für Kontentransaktionen: "Homebanking", Kunde/Versandhaus für Bestellungen: "Homeshopping", Kunde/Netzbetreiber haben muß. Die für jeden Anwendungsfall erforderlichen, in der Regel unterschiedlichen Absprachen zwischen den beteiligten Parteien erschweren die Einführung von Authentifizierungsverfahren.

Der Erfindung liegt die Aufgabe zugrunde, die Vielzahl unterschiedlicher Authentifizierungsverfahren bzw. Verfahrensvarianten zu verringern, deren allgemeine Akzeptanz zu verbessern und die Einführung neuer Anwendungsbereiche zu erschließen bzw. zu beschleunigen.

Die Aufgabe wird erfindungsgemäß gelöst, wie im Kennzeichen des Patentanspruchs 1 beschrieben.

Eine vorteilhafte Weiterbildungsmöglichkeit ist im Kennzeichen des Patentanspruchs 2 beschrieben.

Das vorgeschlagene einheitliche Verfahren ermöglicht es, durch Synergie, also zusammenhängende gemeinsame Erfüllung von mehreren Aufgaben, die Kosten für den einzelnen Anwendungsfall zu verringern, schafft für den Benutzer in verschiedenen Anwendungsfällen gleiche Benutzeroberflächen und erhöht damit die Akzeptanz. Gleichzeitig werden neue Anwendungsbereiche erschlossen und die Einführung neuer Anwendungen beschleunigt.

Es ist besonders vorteilhaft, daß die Authentifizierung in seiner technisch/organisatorischen Dimension als Leistungsmerkmal des Telekommunikationsnetzes selbst gestaltet und verschiedenen Nutzerbeziehungen in gleicher Weise angeboten wird.

Die Erfindung wird nachstehend in einem Ausführungsbeispiel näher beschrieben. Die zugehörige Zeichnung zeigt ein Übersichtsbild der Authentifizierung als Netzdienstleistung.

Realisiert wird das Leistungsmerkmal durch eine zusätzliche Schaltungsanordnung im Netz, die als Authentifizierungsmodul bezeichnet ist und welche die Authentifizierungsangaben vom sendenden Endgerät erhält bzw. auf Anforderung des empfangenden Endgeräts abfragt und nach Prüfung und ggf. Umkodierung an das Zielendgerät weitergibt. Dieser Authentifizierungsmodul

ist aus Sicht der Authentifizierung Kommunikationspartner der beteiligten Endgeräte und somit das Kernstück der Dienstleistung. Diese schließt auch die Definition geeigneter Endeinrichtungen bzw. Endgerätfunktionen oder entsprechender Schnittstellen bzw. Schnittstellen-Elemente zur Anschaltung von Endeinrichtungen zur Unterstützung dieses Leistungsmerkmals an das Netz ein.

Als Formen der Authentifizierung zwischen Anrufer und Netz können grundsätzlich alle gängigen Verfahren wie Codeworte, PIN, Speicherkarten, Prozessorkarten bis hin zur Spracherkennung einzeln oder in beliebigen Kombinationen eingesetzt werden. In gleicher Weise können die bekannten Übertragungsverfahren für den Informationstransfer zwischen den beteiligten Systemkomponenten zum Einsatz kommen.

Eine Ausführungsmöglichkeit der Erfindung ist die Einführung einer Chipkarte entsprechend den bestehenden Standards, die neben den notwendigen Sicherungsalgorithmen zunächst nur Informationen zur Kennzeichnung des Karteninhabers enthält und in der Lage ist, über ein geeignetes Endgerät mit der ergänzenden Schaltungsanordnung im Netz zu kommunizieren.

Zusammen mit entsprechenden Endgeräten stellt diese Karte einen Schlüssel zur Kommunikation über das Authentifizierungsmodul und somit zur Nutzung des entsprechenden Dienstleistungsangebot des Netzbetreibers dar. Die Übermittlung der Authentifizierungsinformation an den Angerufenen erfolgt unter Nutzung bekannter Übertragungsverfahren, sofern dieser am Authentifizierungsdienst des Netzbetreibers teilnimmt. Die Chipkarte kann zusätzlich noch mit anderen Funktionen ausgestattet werden.

Aufbauend auf dem beschriebenen Anwendungsbeispiel können bereits bestehende Kartensysteme in dieses System integriert werden. Hierfür bietet sich z. B. die heute bereits vorhandene "Multifunktionalen Chipkarte" (MFC-Karte) an. Sie kann dann nicht nur in den bestehenden Beziehungen Kunde/Raiffeisen-Bank und Kunde/Telekom (Öffentliches Telefon) benutzt werden, sondern zusätzlich in allen anderen, dem Authentifizierungsdienst angeschlossenen Anwendungen.

Die Aufgabe des Authentifizierungsmoduls besteht in der Hauptsache darin, die Echtheit der Karte, die Nutzungsberechtigung, das Abprüfen von Sperrlisten und die entsprechenden Berechtigungen bzw. Service-Profile des Karteninhabers zu prüfen und in Aktionen, z. B. Informationsübermittlung an den angerufenen Gesprächspartner, umzusetzen.

Die Echtheitsprüfung kann z. B. auf der Basis eines Call-Response-Verfahrens erfolgen. Gegenstand der Prüfung ist in diesem Fall der auf der Chipkarte auf Krypto-Basis enthaltene Algorithmus. Zu realisieren ist der Authentifizierungsmodul als Einrichtung zum Empfangen und Senden von digitalen Informationen entsprechend den im Netz optimalen Übertragungsverfahren. Die Verarbeitung dieser Informationen erfolgt auf Software-Basis.

#### Patentansprüche

1. System zur Authentifizierung von Anrufern, die über Telekommunikationsnetze, vorzugsweise Telefonnetze, Dienste eines Angerufenen in Anspruch nehmen und hierzu ihre persönliche Identität bekanntgeben, dadurch gekennzeichnet, daß die bestimmenden Parameter der Benutzeroberfläche

des Verfahrens der Authentifizierung vom Netzbetreiber festgelegt und in die Netzdienstleistungen einbezogen werden, und daß vereinbarte Modalitäten der Authentifizierung und mit den Vermittlungseinrichtungen verbundene Vorrichtungen dafür, entsprechend den unterschiedlichen Arten der Nutzerbeziehungen zwischen Anrufer und Angerufenem, in Verbindung mit dem Vermittlungsvorgang zur Verfügung gestellt werden. 5

2. System nach Anspruch 1, dadurch gekennzeichnet, daß die Vorgänge des Verbindungsaufbaus mit denen der Authentifizierung in Form der Synergie verknüpft werden. 10

---

Hierzu 1 Seite(n) Zeichnungen

15

20

25

30

35

40

45

50

55

60

65

# Übersichtsbild

